Cybersecurity Automation and Threat Intelligence Sharing Best Practices

April 2021

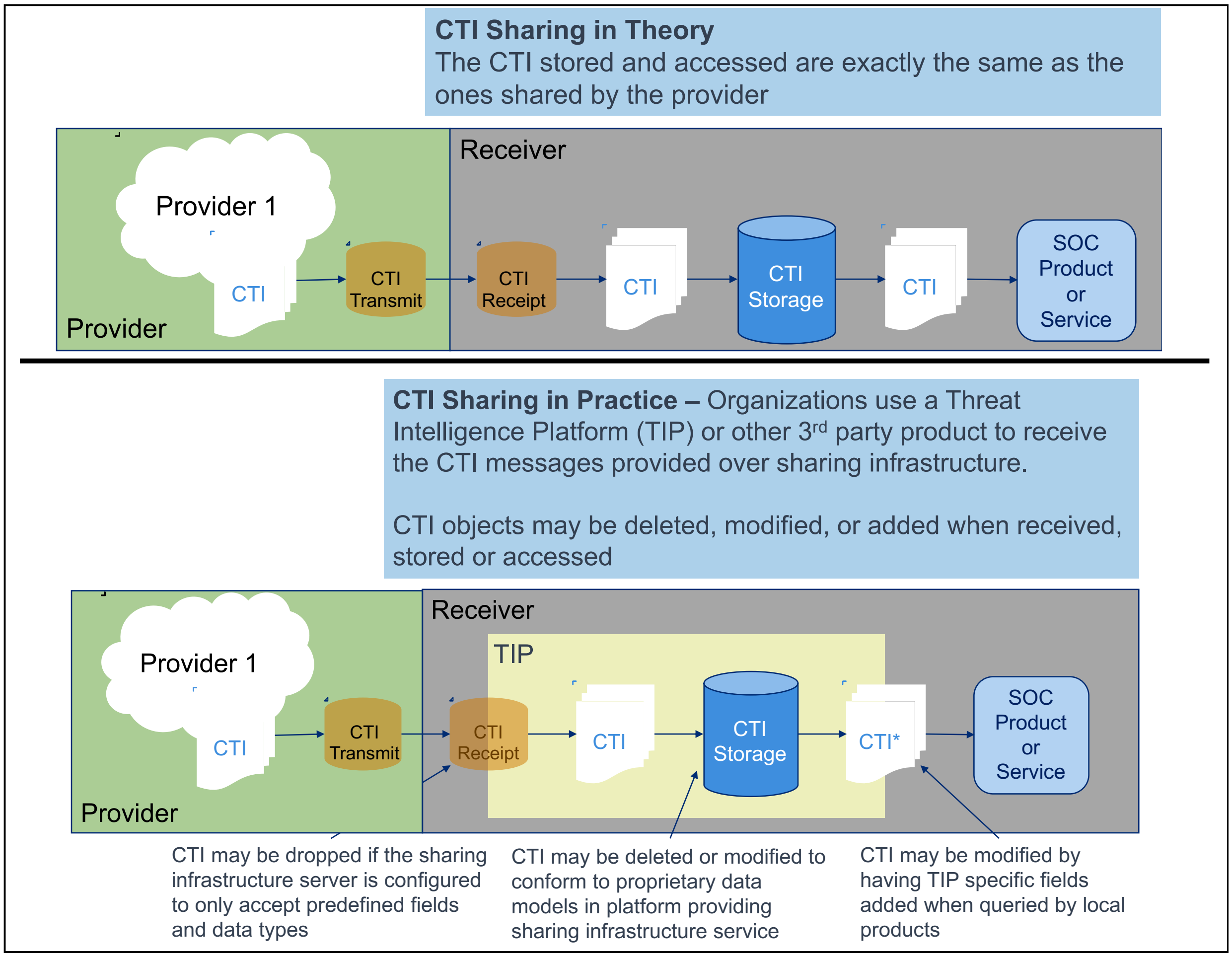
JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

CYBER THREAT INTELLIGENCE (CTI) SHARING INFRASTRUCTURES

Preserving CTI Content

Kimberly K. Watson

Operational limitations have resulted in many organizations deploying 3rd party products to ingest standards-based CTI feeds. Unfortunately, many of these products modify the shared content when they receive it from the producer. Often the methods utilized for CTI delivery through 3rd party sharing infrastructure results in limitations regarding the usefulness of new or unique CTI, and nullifies the expected value of using community accepted standards.



CTI Sharing in Theory
The CTI stored and accessed are exactly the same as the ones shared by the provider

CTI Sharing in Practice – Organizations use a Threat Intelligence Platform (TIP) or other 3rd party product to receive the CTI messages provided over sharing infrastructure.

CTI objects may be deleted, modified, or added when received, stored or accessed

CTI may be dropped if the sharing infrastructure server is configured to only accept predefined fields and data types

CTI may be deleted or modified to conform to proprietary data models in platform providing sharing infrastructure service

CTI may be modified by having TIP specific fields added when queried by local products

Consumers will select CTI sources by how easily they can be incorporated into their environment, not the uniqueness of content. If the content takes too much effort to access or make available to internal products and services, it is not seen as worth the investment.

Sharing infrastructure that results in modification of CTI

The earliest implementations of TAXII infrastructure for CTI sharing relied heavily on the use of STIX profiles. This ensured that only content that had been through the approved sanitization process was shared. Unfortunately, this prevented the receipt of any content not aligned with the profile, which directly limited the CTI that could be shared through this infrastructure. Advancements in the standards have eliminated the profile concept from STIX, but many 3rd party CTI sharing products still follow the same behavior derived from the profile concept. This results in data from a provider that does not meet the sharing infrastructure's expectation is dropped.

While some TIPs differentiate themselves based on unique CTI or member communities, most market some advanced capability to visualize, analyze, correlate, or prioritize threat information from multiple sources. These advanced capabilities are based on proprietary algorithms or models, which often makes how they store the CTI proprietary as well. Most products that import or export threat intelligence have a way to map CTI that they receive from various source messages to their own proprietary data models. As a result content is often dropped or overwritten if the CTI transmission and receipt servers are not provided by the same vendor or sharing organization. This can be compounded by the final receiver of the CTI being unable to easily verify that the CTI they received was modified mid-stream by a 3rd party product. While some organizations prefer having a single source for CTI enrichment, others may have security policies that prefer to know whether information such as confidence was derived from the original sender of the CTI or by the 3rd party product providing sharing infrastructure.

This significantly impacts receiving organizations because they may need to maintain multiple sharing infrastructures to consume feeds from different providers if they wish to be able to discern whether all fields related to their received CTI are original content or modified. Since all the data from these different sources is going into the same platform for storage and/or analysis, organizations are defaulting to using the infrastructure provided by products they have already deployed. They are willing to limit their CTI sources to those that their products and services can consume correctly on their behalf. They will not use more valuable sources if they need to maintain the associated sharing infrastructure themselves.

Alternative Sharing Infrastructures

CTI providers need to develop sharing infrastructures that enable consumers to ingest multiple CTI feeds using capabilities available by default in their environment. Any service provided to ingest CTI needs to ensure that they do not modify, delete, or add content. If such modifications do occur, the final recipient needs an infrastructure that easily allows them to view the original CTI as well as the modified one.

Robust standards, such as STIX2.0 and STIX2.1, have the ability to convey complex insights and relationships. As CTI providers use these standards to enhance their content, it will become even more important that organizations are able to ensure that they are accessing the improved intelligence. By implementing more transparent infrastructures, organizations can gain the most operational value from their CTI investments. They can also ingest and use a new content type as soon as it is available instead of waiting for existing vendors to include that capability on their technology roadmaps.

Conclusion

A key design element of CTI standards such as STIX is to ensure that the data sent is the data received. As 3rd party sharing infrastructures become more prevalent, it is clear that to preserve this intent, the infrastructure must provide a way for the final recipient of CTI to understand what aspects of the CTI have been modified and repackaged before being provided to the final recipient. This issue will become more critical as CTI sharing evolves to include more complex bundles of relationships and where the modification of a single field may have multiple unintended secondary effects to the entire CTI narrative and intent

Acknowledgement

This material is based upon work supported by the U.S. Department of Homeland Security / Cybersecurity and Infrastructure Security Agency under Grant Award Number DHS-19-CISA-128-SLT-001 (State, Local, Tribal, and Territorial Indicators of Compromise Automation Pilot).

Disclaimer

The views and conclusions contained in this document are those of the author and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security / Cybersecurity and Infrastructure Security Agency.